UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/708,397	11/08/2000	Roger Kenneth Abrams	RPS920000077US1	2446

25299 7590 01/15/2004

IBM CORPORATION
PO BOX 12195
DEPT 9CCA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	5

DATE MAILED: 01/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/708,397	ABRAMS, ROGER KENNETH	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (US 6,647, 400 B1).

a. *Referring to claim 1:*

i. Moran teaches:

(1) a bus system **[i.e., referring to Figure 1, bus 114 can be used to provide access other subsystems and devices as well (column 6, lines 13-14). In addition, bus 114 is illustrative of any interconnection scheme serving to link the subsystems (column 7, lines 12-14)]**;

(2) a CPU connected to the bus system **[i.e., referring to Figure 1, In addition to providing CPU 102 access to storage subsystems, bus 114 can be used to provide access other subsystems and devices as well (column 6, lines 12-14)]**;

(3) a RAM connected to the bus system, the RAM being divided into pages, each page having an execution flag **[i.e., referring to Figure 1, CPU 102 is coupled bidirectionally with memory 110, via bus 114, which can include a first primary storage, typically a random access memory (RAM), and a second primary storage area, typically a read-only memory (ROM), whereby "the RAM being divided into pages, each page having an execution flag" is considered to include within memory 110]**;

(4) a memory manager configured to manage the pages of the RAM and permit CPU execution of data on pages according to the execution flag **[i.e., referring to Figure 1, "a memory manager" is considered to include in memory 110 for "configuring to manage the pages of the RAM and permit CPU execution of data on pages according to the execution flag"];**

(5) a program stored within at least one page of the RAM **[i.e., a primary storage, typically a random access memory (RAM), can also store programming instructions and data, in the form of data objects and text objects, in addition to other data and instructions for processes operating on CPU 102 (column 5, lines 49-52)]**; and

(6) a program stack stored within at least one page the RAM **[i.e., most buffer overflow exploits involving overwriting the control information on the process's stack, in which "a program stack" stored in memory 110 (column 34, 29-28)]**,

(7) wherein the memory manager is configured to determine whether the program is susceptible to buffer overflow attacks, and, if so, set the execution flag for program stack pages of RAM to deny CPU execution of data on the program stack pages of RAM **[i.e., referring to Figure 1, "the memory manager" is considered to include in memory 110 for "configuring to determine whether the program is susceptible to buffer overflow attacks". Currently, the most common exploits involve a buffer overflow attacks on SetUID commands. A SetUID (also "SUID") command is one that runs with the privileges of the owner of the command instead of with the privileges of the user invoking the commands, and this attribute is specified by a flag in the permissions for the command (an executable file) (column 33, lines 64-67 through column 34, lines 1-3). Almost all buffer overflows attack take effect at the very beginning of the execution of the program, because the data causing the overflow is supplied as part of the command invocation or setup. Hence, the command is subverted (replaced) before it has a chance to perform any of its intended actions. This observation is**

key to the approach used in an embodiment of the invention to detect buffer overflow attacks ex post facto (column 34, lines 43-50)].

b. *Referring to claim 2:*

i. Moran further teaches:

(1) wherein the memory manager and the CPU are configured to deny CPU execution of data by triggering a hardware interrupt **[i.e., referring to Figure 1, CPU 102 is coupled bidirectionally with memory 110, in which "the memory manager" is considered to include in memory 110. It can also store programming instructions and data, that is "a hardware interrupt", in the form of data objects and text objects, in addition to other data and instructions for processes operating on CPU 102. Primary storage typically includes basic operating instructions, program code, data and objects used by the CPU 102 to perform its functions, that is "to deny CPU execution of data" (column 5, lines 43-55)].**

c. *Referring to claim 3:*

i. Moran further teaches:

(1) a process structure table in data communication with the memory manager, wherein the memory manager comprises an annotation API, wherein the annotation API is configured to annotate within the process structure table the susceptibility of the program to buffer overflow attacks, and wherein the memory manager is configured to make the determination of susceptibility to buffer overflow attacks with reference to the process structure table **[i.e., referring to Figure 1, the memory can also store programming instructions and data, that is "a process structure table", in the form of data objects and text objects, in addition to other data and instructions for processes operating on CPU 102. Primary storage typically includes basic operating instructions, program code, data and objects used by the CPU 102 to perform its functions, wherein "the memory manager" and "an annotation API" are part of the memory which "is configured to annotate within the process structure table the susceptibility of the program to buffer overflow attacks" and "is configured to make the determination of susceptibility**

to buffer overflow attacks with reference to the process structure table" (column 5, lines 43-55)].

d. *Referring to claims 4, 5, 20, and 21:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

e. *Referring to claims 6, 7, and 8:*

i. These claims have limitations that is similar to those of claims 1 and 3, thus they are rejected with the same rationale applied against claims 1 and 3 above.

f. *Referring to claim 9:*

i. Moran teaches:

(1) a memory manager code comprising a set of codes operable to direct a data processing system to manage a set of pages within a RAM of the data processing system and to permit a CPU of the data processing system to execute data on pages according to an execution flag on each of the set of pages; an application program code comprising a set of codes operable to direct a data processing system to request the memory manager code to establish a program stack within at least one page the RAM; and a susceptibility code comprising a set of codes operable to direct a data processing system to determine whether the application program code is susceptible to buffer overflow attacks, and, if so, set the execution flag for the program stack pages to deny CPU execution of data on the program stack pages **[i.e., referring to Figure 1, memory 110 which can include primary storage for storing basic operating instructions, program code, data and objects used by the CPU 102 to perform its functions (column 5, lines 43-55). In addition, embodiments of the present invention further relate to computer storage products with a computer readable medium that contain program code (that is "a memory manager code, an application program code, and a susceptibility code") for performing various computer-implemented operations (column 6, lines 52-55). The computer-readable medium can also be distributed as a data signal embodied in a carrier wave over a network of coupled computer systems so that**

the computer-readable code is stored and executed in a distributed fashion. Examples of program code include both machine code, as produced, for example, by a compiler, or files containing higher-level code that may be executed using an interpreter (column 7, lines 2-8)].

g. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

h. *Referring to claims 11 and 12:*

i. These claims have limitations that is similar to those of claims 3 and 9, thus they are rejected with the same rationale applied against claims 3 and 9 above.

i. *Referring to claims 13 and 14:*

i. Moran further teaches:

(1) wherein the memory manager code comprises the process structure table code as an API **[i.e. the computer storage products with a computer readable medium that contain program code (that is "a memory manager code, an application program code, and a susceptibility code") for performing various computer-implemented operations (column 6, lines 52-55), whereby "the process structure table code as an API" is considered to include in the program code].**

j. *Referring to claims 15, 16, and 17:*

i. Moran further teaches:

(1) wherein the application program code further comprises a set of codes operable to direct a data processing system to call the process structure table code the application program code is susceptible to buffer overflow attacks **[i.e. the computer storage products with a computer readable medium that contain program code (that is "a memory manager code, an application program code, and a susceptibility code") for performing various computer-implemented operations (column 6, lines 52-55), whereby "a set of codes operable to direct a data processing system to call the process structure**

table code the application program code is susceptible to buffer overflow attacks" is considered to include in the program code], and

(2) the memory manager code further comprises a set of codes operable to direct a data processing system to determine susceptibility upon receipt of a request to allocate an additional page of RAM for the application program code **[i.e. the computer storage products with a computer readable medium that contain program code (that is "a memory manager code, an application program code, and a susceptibility code") for performing various computer-implemented operations (column 6, lines 52-55), whereby "a set of codes operable to direct a data processing system to determine susceptibility upon receipt of a request to allocate an additional page of RAM for the application program code" is considered to include in the program code].**

k. *Referring to claim 18, 24, and 25:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

l. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claims 1 and 2, thus it is rejected with the same rationale applied against claims 1 and 2 above.

m. *Referring to claims 20 and 21:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

n. *Referring to claims 22 and 23:*

i. This claim has limitations that is similar to those of claims 3 and 9, thus it is rejected with the same rationale applied against claims 3 and 9 above.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Yarom (US 5, 949, 973) discloses a stack override prevention method provides protection against a computer attack that utilizes the technique of stack override to gain control of a computer system (see abstract).

b. Moudgill (US 6, 578, 094) discloses a method that allows a called procedure to determine a "safe" upper bound value representing the amount of data that can be written to a stack allocated array/buffer without overwriting any stack-defined data stored in reserved memory blocks in the stack (i.e., any region in memory that is preserved by a calling sequence) (see abstract).

c. Sober (US 6, 088,777) discloses a memory manager requests a large area of memory from an operating system, and from the viewpoint of the operating system, that memory is fixed. That fixed memory area is then divided up into an integral number of classes, e.g. by the memory manager (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
January 8, 2004

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER 2